IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	:	
Rieko ASAI et al.	:	
Serial No. NEW	:	**Attn: APPLICATION BRANCH**
Filed July 31, 2003	:	Attorney Docket No. 2003_1060A

APPARATUSES AND METHODS FOR DECRYPTING ENCRYPTED DATA AND LOCATING THE DECRYPTED DATA IN A MEMORY SPACE USED FOR EXECUTION

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-225289, filed August 1, 2002, Japanese Patent Application No. 2002-359072, filed December 11, 2002, and Japanese Patent Application No. 2003-157255, filed June 2, 2003, as acknowledged in the Declaration of this application.

Certified copies of said Japanese Patent Applications are submitted herewith.

Respectfully submitted,

Rieko ASAI et al.

By _____
Jeffrey R. Filipek
Registration No. 41,471
Attorney for Applicants

JRF/kjf
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 31, 2003

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　８月　１日

出願番号
Application Number: 特願２００２－２２５２８９

[ST.10/C]: [ＪＰ２００２－２２５２８９]

出願人
Applicant(s): 松下電器産業株式会社

２００３年　６月２０日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０４８６９６

【書類名】　特許願
【整理番号】　2032740020
【提出日】　平成14年 8月 1日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 9/00
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　浅井　理恵子
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　庄田　幸恵
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　廣田　照人
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100090446
【弁理士】
【氏名又は名称】　中島　司朗
【手数料の表示】
【予納台帳番号】　014823
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9003742

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　暗号化データ復号方法およびその装置

【特許請求の範囲】

【請求項１】　単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、メモリ空間上の配置位置を保持するメモリ配置情報保持部と、

前記プログラムの記憶装置上の位置情報を保持するアドレステーブル情報保持部と、

暗号化されたデータを暗号鍵に基づき復号する暗号化データ復号部と、

上記暗号鍵を保持する暗号鍵保持部と、

前記暗号化データ復号部に復号指示を出し、前記アドレステーブル情報保持部が保持する情報に従って前記プログラムを記憶装置上から読み出し、暗号化された前記プログラムを復号して、前記メモリ配置情報保持部が保持するメモリ空間上の配置位置にロードする制御部と、

を有することを特徴とする暗号化データ復号方法およびその装置。

【請求項２】　単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、メモリ空間上の配置位置を暗号化して保持するメモリ配置情報保持部と、

前記プログラムの記憶装置上の位置情報を保持するアドレステーブル情報保持部と、

暗号化されたデータを暗号鍵に基づき復号する暗号化データ復号部と、

前記暗号化されたメモリ配置情報保持部の配置情報を暗号鍵に基づき復号する暗号化情報復号部と、

上記暗号鍵を保持する暗号鍵保持部と、

前記暗号化されたメモリ配置情報保持部の配置情報を復号する暗号化情報復号部と、

前記暗号化データ復号部と前期暗号化情報復号部に復号指示を出し、前記アドレステーブル情報保持部が保持する情報に従って前記プログラムを記憶装置上から読み出し、暗号化された前記プログラムを復号し、前記メモリ配置情報保持部が保持する暗号化された情報を前記暗号化データ復号部が復号し、復号された情

報に従ってメモリ空間上の配置位置にロードする制御部と、
を有することを特徴とする請求項１記載の暗号化データ復号方法およびその装置。

【請求項３】　単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、メモリ空間上の配置位置を保持するメモリ配置情報保持部と、
前記プログラムの記憶装置上の位置情報を暗号化して保持するアドレステーブル情報保持部と、
暗号化されたデータを暗号鍵に基づき復号する暗号化データ復号部と、
前記暗号化されたアドレステーブル情報保持部の位置情報を暗号鍵に基づき復号する暗号化テーブル情報復号部と、
上記暗号鍵を保持する暗号鍵保持部と、
前記暗号化データ復号部と前記暗号化テーブル情報復号部に復号指示を出し、前記暗号化データ復号部が復号した前記アドレステーブル情報保持部が保持する情報に従って前記プログラムを記憶装置上から読み出し暗号化された前記プログラムを復号して、前記メモリ配置情報保持部が保持するメモリ空間上の配置位置にロードする制御部と、
を有することを特徴とする請求項１記載の暗号化データ復号方法およびその装置。

【請求項４】　プログラム実行中に割り込みにより不正に処理の流れを奪われた場合に、それを検知し対抗措置をとる不正アクセス防止部を追加したこと、を特徴とする請求項1または２または３記載の暗号化データ復号方法およびその装置。

【請求項５】　前記暗号化データ復号部または前記暗号化情報復号部または前記暗号化テーブル復号部がデータを復号する際に実行する復号支援プログラムが正当なものであるか否かを認証する復号支援プログラム認証部を追加したこと、を特徴とする請求項1または２または３または４記載の暗号化データ復号方法およびその装置。

【請求項６】　前記メモリ配置情報保持部の保持するメモリ空間上の配置位置をプログラム生成時にあらかじめ定義するメモリアドレス定義部を追加したこ

と、を特徴とする請求項1記載の暗号化データ復号方法およびその装置。

【請求項７】　前記アドレステーブル情報保持部が保持するアドレスの情報が正当なものか否かを判定するアドレス情報認証部を追加したこと、を特徴とする請求項1記載の暗号化データ復号方法およびその装置。

【請求項８】　プログラムを実行する際に予め定められたメモリ空間上のメモリアドレス範囲内にプログラムを展開し実行する制御部を有すること、を特徴とする請求項1記載の暗号化データ復号方法およびその装置。

【請求項９】　前記制御部は、単位毎に分割されたプログラムをコンピュータシステムのメモリ空間上に配置する際に、既に他のプログラムが配置されている場合は一旦消去し、上書きすることを特徴とする請求項1記載の暗号化データ復号方法およびその装置。

【請求項１０】　前記データ復号部に復号指示を出し、前記アドレステーブル情報保持部が保持する情報に従って前記メモリ配置情報保持部が保持するメモリ空間上の配置位置に従って単位毎にコンピュータシステムのメモリ空間上にプログラムを配置しながら実行する制御プログラム自身を、予め定められたメモリ空間上のメモリアドレス範囲内にロードし実行するプログラム実行部を有すること、を特徴とする請求項６または７記載の暗号化データ復号方法およびその装置。

【請求項１１】　プログラム実行中に割り込みにより不正に処理の流れを奪われた場合に、プログラムの実行を中断させるトラップ命令を発行する不正アクセス防止部を追加したこと、を特徴とする請求項1記載の暗号化データ復号方法およびその装置。

【請求項１２】　プログラムの逆解析を実行するステップを検出し、逆解析を中断させる逆解析防止部を追加したこと、を特徴とする請求項1記載の暗号化データ復号方法およびその装置。

【請求項１３】　前記不正アクセス防止部は、前記逆解析防止部が動作している際には動作を一時的に中断させること、を特徴とする請求項２記載の暗号化データ復号方法およびその装置。

【請求項１４】　前記メモリ配置情報保持部の保持するメモリ空間上の配置

位置をプログラム生成時にあらかじめ定義するメモリアドレス定義部と、

前記メモリアドレス定義部が定義した情報に基づいて単位毎に分割され暗号化されたプログラムを生成するプログラム生成部とを有すること、を特徴とする暗号化データ復号方法およびその装置。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】

本発明は、実行プログラムの逆解析や不正使用を防止する暗号化データ復号方法およびその装置に関する。

【０００２】

【従来の技術】

従来、暗号方式をコンピュータシステムに提供し、暗号化されたプログラムやデータを復号して利用する場合には、そのシステムの上で動作する復号プログラムを実行する。このとき、仕様が公開されたオープンなコンピュータシステムに置いては、プログラムの解析および改変が容易であるため、復号プログラムを改変することにより、もとの復号プログラムの仕様に反して、復号したデータを不正に利用することが簡単にできてしまい、システム全体の安全性は低くなるという問題があった。

【０００３】

この問題を解決しようとする提案として、復号プログラム自体を暗号化し、データ復号時にのみ復号プログラムを復号して、データ復号作業を行う手段を採用し、これにより、復号プログラムの解析および改変を困難にするものが知られている。（特開平９－６２３２）。しかし、復号プログラムを復号するプログラムの解析、および改竄が成功すると、改竄プログラムの実行を防ぐことはできない。これに対し、復号プログラムの正当性を暗号化データの復号時に認証できるようにし、改竄された復号プログラムによる意図しない目的への復号したデータの流用を防止する提案がある（特開平１１－３９１５６）。

【０００４】

ところが、正当性が証明された復号プログラムを実行する場合には、コンピュ

ータシステム上のメモリに復号された状態でプログラムがロードされる。このときに、不正な割り込み等により処理の流れを横取りされると、全てのプログラムが覗き見されてしまう。

また、メモリ上へのプログラムのロード方法として、オーバーレイリンカ／ローダが知られている（Ｌｉｎｋｅｒｓ＆Ｌｏａｄｅｒｓ　Ｊｏｈｎ　Ｒ．Ｌｅｖｉｎｅ　オーム社　ｐ１６５）。オーバレイは、プログラムサイズよりも小さいメモリにプログラムを収めるために使われる手法である。プログラムのコードを小さなサイズでセグメント分割する。オーバレイのいくつかのセグメントは、同じメモリを共有する。プログラムが起動するとき、システムは、プログラムのエントリポイントを持つセグメントをロードする。オーバレイローダは、呼び出し先へのパスが含まれる各セグメントを、必要に応じて随時、ロードする。

【０００５】

しかし、従来のオーバレイリンカ／ローダでは、必要なセグメントを必要な時に順に限られた大きさのメモリ上にロードし、要らなくなったときに削除、または、他のプログラムが上書きすることによって消去されるため、メモリ上にプログラムのコードやデータが残されたままの状態になってしまうという問題があった。また、オーバーレイローダがプログラムをロードするアドレスが固定されるため、プログラムへのアクセスが容易に解読できてしまうという問題があった。

【０００６】

以上のように、従来の技術では、一般的なコンピュータシステムにおいては、復号プログラムがメモリ上にロードされているときに不正な割り込みが発生した場合、全てのプログラムが覗き見されてしまい、復号プログラムのアルゴリズムや暗号鍵が暴露されてしまう。また、近年のコンピュータシステムは、メモリに制約を持たないのでオーバレイの手法を用いることはほどんどなく、プログラム全体をメモリ上に展開している。このため、システム全体の安全性が低くなってしまうという問題がある。

【０００７】

【発明が解決しようとする課題】

本発明は、仕様が公開されているオープンなコンピュータシステムにおいても

、プログラムを部分的に復号しながらメモリ上にロードできるようにすることにより、不正な割り込み等で処理の流れが横取りされても、メモリ上からプログラムの全体を覗き見を防止することを課題としている。

【０００８】

【課題を解決するための手段】

この課題を解決するために、本発明は、単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、メモリ空間上の配置位置を保持するメモリ配置情報保持部と、前記プログラムの記憶装置上の位置情報を保持するアドレステーブル情報保持部と、暗号化されたデータを暗号鍵に基づき復号する暗号化データ復号部と、上記暗号鍵を保持する暗号鍵保持部と、前記暗号化データ復号部に復号指示を出し、前記アドレステーブル情報保持部が保持する情報に従って前記プログラムを記憶装置上から読み出し、暗号化された前記プログラムを復号して、前記メモリ配置情報保持部が保持するメモリ空間上の配置位置にロードする制御部とを備えたものである。

【０００９】

【発明の実施の形態】

次に本発明の第一の実施例について図面を用いて説明する。図１は、本発明の暗号化データ復号方法およびその装置の構成を示す機能ブロック図である。図１においてメモリ配置情報保持部１０４は単位毎に分割されたプログラムを実行する際にメモリ空間上の配置位置を示す情報を保持し、アドレステーブル情報保持部１０３は、分割されたプログラムがメモリ上のどの位置に格納されているかという情報を暗号化して保持している。また暗号化データ復号部１０２は、暗号化されたデータを暗号鍵に基づき復号し、暗号鍵保持部１０１は暗号化データ復号部１０２が暗号化データを復号化する際に用いる暗号鍵を保持し、またアドレス情報認証部１０５は、アドレステーブル情報保持部１０３が保持する情報が正当なものか否かを認証し、メモリアドレス定義部１０８はメモリ配置情報保持部１０４の保持するメモリ空間上の配置位置をプログラム生成時にあらかじめ定義する。不正アクセス防止部１０７は、プログラム実行中に割り込み等により不正に処理の流れを奪われた場合に、それを検知し対抗措置をとる。さらに復号支援プ

ログラム認証部１００は前記暗号化データ復号部１０２が暗号化されたデータを復号する際に用いる復号支援プログラムが正当なものか否かを認証する。制御部１０６は、暗号化データ復号部１０２に復号指示を出し、前記アドレステーブル情報保持部１０３が保持する情報に従って前記メモリ配置情報保持部が保持するメモリ空間上の配置位置に従って単位毎にコンピュータシステムのメモリ空間上にプログラムを配置しながら実行する。

【００１０】

図２は、制御部１０６が配置するメモリ配置構成の概念図である。

図３は、メモリ配置情報保持部１０４が保持する暗号化されたアドレス情報および復号化されたアドレス情報およびハードディスク上のイメージ図であり、

図４はメモリ配置情報保持部１０４が保持するメモリ空間上の配置位置を示す情報の概念図である。

【００１１】

上記のような構成の暗号化データ復号方法およびその装置において単位毎に分割されたプログラムのロード処理の具体的な流れを図５を用いて説明する。

ここでいうプログラムのロードとは、プログラムを実行できるようにハードディスクのような2次記憶装置からメインメモリにコピーすることである。また単位毎に分割されたプログラムとは、１つのソースファイルまたは関連するソースファイルのグループから生成されたオブジェクトコードを指している。このオブジェクトコードとは具体的には一つのプログラムを構成する一部分を示すサブプログラムであったりあるいはライブラリモジュールそのものを指している。

＜プログラムのロード手順＞

１．　制御部１０６は、暗号化テーブル情報復号部１１０に対してデータを復号化するよう指示を出し、（Ｓ５０１）続いてロードすべきプログラムＡが格納されているアドレスの情報を取得するためにアドレステーブル情報保持部１０３の情報を読み出す（Ｓ５０２）

２．　暗号化テーブル情報復号部１１０は、制御部１０６から復号指示を受け取ると、データを復号する際に実行する復号支援プログラムが正当なものであるか否かを認証する。（Ｓ５０３）この認証処理に用いる情報の例として、プログ

ラムのサイズ、更新日時、あるいはプログラムの一方向ハッシュ値を用いて元の復号支援プログラムが実行時に改ざんされていないかを認証する。もちろん、この認証手段は電子署名認証技術などの一般に公開されている技術を用いてもよい。

【００１２】

３．　２．で認証に成功した場合、暗号化テーブル情報復号部１１０は、図３の（３－１）に示すようなデータを暗号鍵保持部１０１が保持している暗号化されたデータを復号するための鍵に基づき読み出したデータを復号し（Ｓ５０４）、プログラムＡが格納されている図３の（３－２）に示すようなアドレスの情報を得る。もし２．で認証に失敗した場合、暗号化テーブル情報復号部１１０はデータの復号を行わずプログラムの処理を中断し（Ｓ５１７）、制御部１０６は、メモリ空間上に復号されたデータがロードされている場合は消去する。（Ｓ５１８）

４．　続いてアドレス情報認証部１０５は、３．で得たアドレス情報が正当なものであるか否かを認証する。（Ｓ５０５）この認証には、２の認証処理で用いたものと同じ一方向ハッシュ関数等、一般に用いられている認証技術を用いる。アドレス情報認証部１０５がアドレス情報が正当なものであると認証した場合に、ステップ５．に進み、認証に失敗した場合は、制御部１０６はプログラムの処理を中断し、（Ｓ５１７）メモリ空間上にデータがロードされている場合は消去する。（Ｓ５１８）

５．　引き続き制御部１０６は、暗号化データ復号部１０２に指示を出す。（Ｓ５０６）

６．　暗号化データ復号部１０２は、制御部１０６から復号指示を受け取ると、データを復号する際に実行する復号支援プログラムが正当なものであるか否かを認証する。（Ｓ５０７）この認証処理に用いる情報の例として、プログラムのサイズ、更新日時、あるいはプログラムの一方向ハッシュ値を用いて元の復号支援プログラムが実行時に改ざんされていないかを認証する。もちろん、この認証手段は電子署名認証技術などの一般に公開されている技術を用いてもよい。

【００１３】

７．　６．で認証に成功した場合、図３の（３－３）に示すようなハードディスクの該当のアドレス位置から読み出したプログラムＡを読み出す。（Ｓ５０８）暗号化データ復号部１０２は読み出された暗号化されたプログラムＡを復号する。（Ｓ５０９）６．で認証に失敗した場合、データの復号を行わずプログラムの処理を中断し（Ｓ５１７）、制御部１０６は、メモリ空間上に復号されたデータがロードされている場合は消去する。（Ｓ５１８）

８．　さらに制御部１０６は、暗号化情報復号部１０９に復号指示を出す。（Ｓ５１０）

９．　暗号化情報復号部１０９は、制御部１０６から復号指示を受け取ると、データを復号する際に実行する復号支援プログラムが正当なものであるか否かを認証する。（Ｓ５１１）この認証処理に用いる情報の例として、プログラムのサイズ、更新日時、あるいはプログラムの一方向ハッシュ値を用いて元の復号支援プログラムが実行時に改ざんされていないかを認証する。もちろん、この認証手段は電子署名認証技術などの一般に公開されている技術を用いてもよい。

【００１４】

１０．９．で認証に成功した場合、暗号化情報復号部１０９はメモリ配置情報保持部１０４が保持する図４に示すようなメモリ空間上の配置位置情報の情報を読み出し、（Ｓ５１３）読み出されたメモリ空間上の配置位置情報を復号化し（Ｓ５１４）、復号化された配置位置情報に従ってプログラムＡを予め定められたメモリ空間上のOS1-1というアドレス空間にロードする。（Ｓ５１５）９．で認証に失敗した場合、配置情報の復号化は行わずに、プログラムの処理を中断し、（Ｓ５１７）制御部１０６は、メモリ空間上に復号されたデータがロードされている場合は消去する。（Ｓ５１８）

１１．制御部１０６は、プログラムＡが呼び出す順に分割されたプログラムＢ～プログラムＩを１．～４．の手順を繰り返すことによりロードする。（おわり）

上記に述べたステップの暗号鍵情報保持部１０１は、具体的には例えばDESのような暗号化方式に用いる暗号鍵を持ち、通常、プログラムの一定領域に埋め込まれるかあるいはユーザには見えない部分あるいはファイルに秘匿されている。

もちろん、暗号方式はこれ以外のものでもよい。簡易化する方法として、単に値の排他的論理和を取る方法等でもよい。また秘匿の方法もこれに限るものではない。

【００１５】

また、暗号化データ復号部１０２、暗号化テーブル情報復号部１１０、暗号化情報復号部１０９は同じものであっても構わないし、異なるものであってもよい。

次に上記１～５の処理ステップの途中で不正アクセス防止部１０７が割り込みにより不正に処理の流れを奪われた場合の処理について第２の実施例を用いて説明する。

【００１６】

割り込みとは、CPU がプログラムを実行している最中に何か重要なイベントが発生することである。一般的にCPU はこの割り込みが発生するとプログラムを一時的に中断し、イベントの処理を行う。この機能を悪用すれば、対象となるプログラムの動作を追跡するために、任意の箇所で停止させ、その状態でのメモリやレジスタの内容を参照したり、あるいは変更して実行を続行させたりすることが可能になる。

【００１７】

具体的な例として、上記ステップ２を実行した後でこの、割り込みを発生させ、プログラムの処理を一時中断すると、復号化されたメモリアドレスの情報が参照でき、また同様に上記ステップの５を実行した後で割り込みを発生させると、メモリ上に展開されたプログラムの内容が参照可能になる。

不正アクセス防止部１０７は、割込みを検知した場合、上記各ステップを中止し、暗号化データ復号部が復号したデータがある場合はメモリ上から消去し、メモリ空間上ロードされてプログラムは消去する。不正アクセス防止部１０７が行う具体的な処理を下記に示す。

【００１８】

１．　不正アクセス防止部１０７は、割り込みを検知すると、プログラムの処理を中断させるトラップ命令を発行し、ＣＰＵのＩＤＴ（Interrupt Descriptor

Table）を参照する。

２．　ＩＤＴテーブルには割り込み命令に対応したハンドラの情報が定義されている。本実施例では、プログラムの中止、メモリ内容の消去といった動作を実行するためのハンドラが定義されている。

【００１９】

３．　不正アクセス防止部１０７は定義されているハンドラに処理を移し、プログラムの中断、メモリ内容の消去が実行される。

また不正アクセス防止部１０７が、プログラムの逆解析を実行するステップを検出する処理について述べる。プログラムの逆解析には、一般に市販されているデバッガ等を用いることにより行える。このデバッガを使えばプログラムが終了する前に停止させたり、問題のあるプログラムを調査して何が悪いのかを調べたりすることができることから、プログラムの改ざん、不正使用の手段として用いられる可能性がある。

【００２０】

このようなデバッガの機能を用いてプログラムの内容が覗かれることを検出する手段の一つとして、デバッガの機能の一つである、ブレイクポイントを用いる。ブレイクポイントを用いると、プログラム内のある特定の箇所に到達するたびに、プログラムを停止することができる。またブレイクポイントにおいてプログラムを停止させるためには満足されなければならない、詳細な条件を設定することもできる。

【００２１】

このデバッガの基本機能を用いて、不正アクセス防止部１０７は、プログラムの逆解析の検出を下記のような手順で行う。

１．　不正アクセス防止部１０７が既にプログラムの逆解析検出ステップが実行されているか否かをチェックする。

２．　既に逆解析検出を実行している場合、同時に２つの監視は行わなくてよいものと判断して何もおこなわない。

【００２２】

３．　２．でまだ逆解析検出ステップが実行されていないと判断した場合は、不正アクセス防止部１０７はプログラム実行前に予め、複数のブレイクポイントを設定し、設定したブレイクポイントの位置情報（行番号、関数名、アドレス等が用いられる）を保持しておく。

４．　プログラム実行時、不正アクセス防止部１０７は１．で保持したブレイクポイントの情報を読み出し、設定した通りの位置でブレイクされるかを監視し、正しい位置でブレイクされた場合はプログラムを再開させる。

【００２３】

５．　予め設定した通りの位置でブレイクされない場合は、不正に他のプロセスによってプログラムが逆解析されているものとして、プログラムの実行を中断し、メモリ内容の消去を実行する。

次にメモリアドレス定義部１０８の処理について述べる。

【００２４】

メモリアドレス定義部１０８はメモリ配置情報保持部１０２が保持する図４に示すようなメモリ空間上の配置位置の情報を、プログラム生成時にあらかじめ定義するものである。プログラムをあらかじめ決まったアドレスのロードするためには、通常プログラム生成時にリンクという処理を行う必要がある。また、複数のプログラムが同じメモリを共有するためには、オーバーレイリンクという技術を用いる。

【００２５】

まず、プログラマは、メモリ空間上のサイズと、各分割されたプログラムのサイズからメモリ空間上の配置位置をレイアウトする。レイアウトする際に、下記のような情報を用いてレイアウトを設計する。

１．　単位毎のプログラムのサイズ

２．　ある単位プログラムがどの単位プログラムをコールするかの主従関係とコールする回数

３．　単位プログラムの秘匿性の高さ

４．　パフォーマンス

このような条件から、メモリ空間上に配置する際、例えばプログラムのパフォーマンスを重視する場合は、プログラムが共有するメモリ空間上の領域は極力小さくする。なぜなら、プログラムをロードし、上書きする回数が多くなればなるほど、パフォーマンスは悪くなるからである。逆にプログラムの秘匿性を高くしたければ、常にメモリ空間は共有し、プログラム単位毎に上書きさせるとよい。

【００２６】

メモリアドレス定義部１０８に入力すると、メモリアドレス定義部１０８は図４に示すようなメモリの配置位置情報に変換する。

ここでメモリアドレス定義部１０８に渡す情報は、手作業でプログラマが設計してもよいし、プログラムのセグメントのヘッダ情報に書かれている情報から自動的に読み出して配置する方法でもよい。

【００２７】

次にプログラム生成部１１１の処理について述べる。

通常ソースコードや、ライブラリの集合から実行形式のプログラムを生成する際にはコンパイラが用いられる。本実施例のプログラム生成部１１１は、プログラムをコンパイルする際に、図４に示すようなメモリアドレス定義部１０８で定義されたメモリ空間上の配置位置にロードされるようにプログラム生成時に定義しプログラムを生成する。

【００２８】

【発明の効果】

以上、説明したように本発明は、プログラムを部分的に復号しながらメモリ上にロードできるようにすることにより、不正な割り込み等で処理の流れが横取りされても、メモリ上からプログラムの全体を覗き見を防止する。これにより、暗号鍵や復号プログラムを盗まれないようにすることができ、安全性なシステムを得ることができる。

【図面の簡単な説明】

【図１】　暗号化データ復号方法およびその装置の構成を示す機能ブロック図。

【図２】　制御部が配置するメモリ配置構成の概念図。

【図３】　メモリ配置情報保持部が保持する暗号化されたアドレス情報および復号化されたアドレス情報およびハードディスク上のイメージ図。

【図４】　メモリ配置情報保持部が保持するメモリ空間上の配置位置を示す概念図。

【図５】　ロード処理を表すフローチャート。

【符号の説明】

１００　復号支援プログラム認証部

１０１　暗号鍵保持部

１０２　暗号化データ復号部

１０３　アドレステーブル情報保持部

１０４　メモリ配置情報保持部

１０５　アドレス情報認証部

１０６　制御部

１０７　不正アクセス防止部

１０８　メモリアドレス定義部

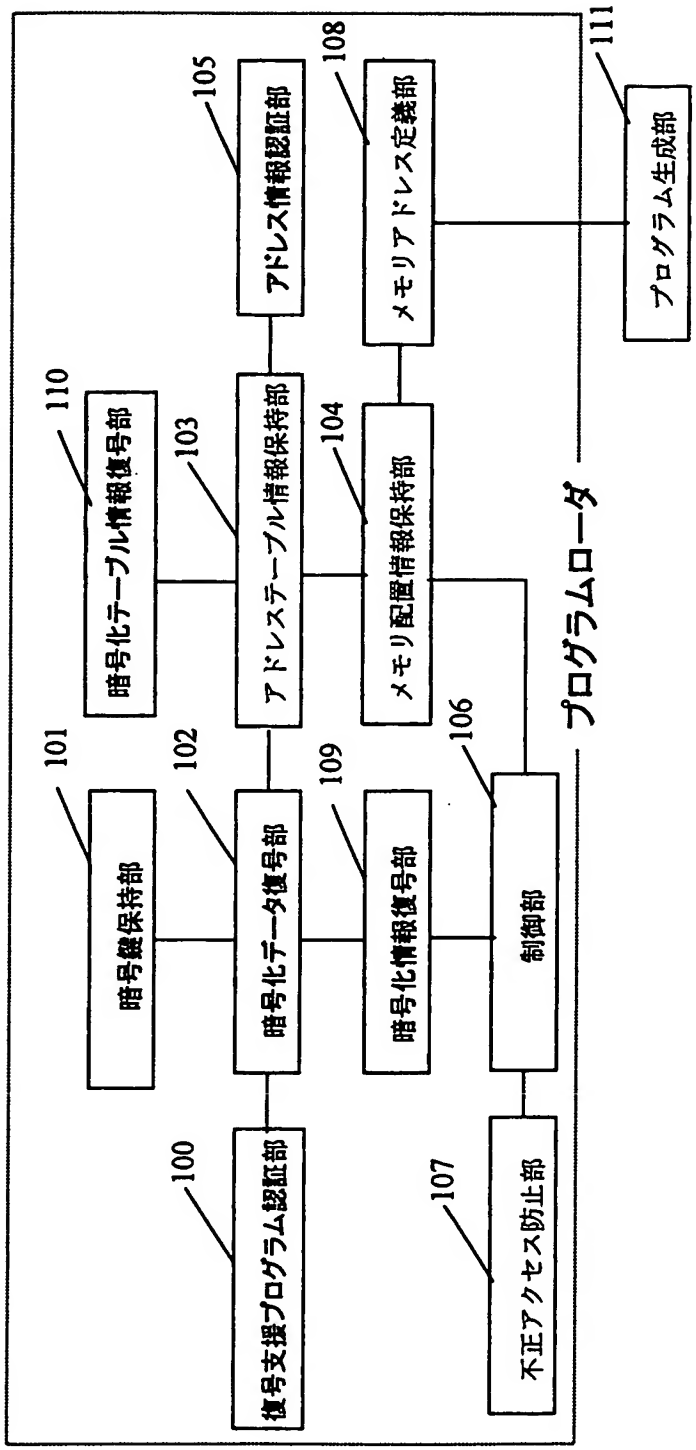
１０９　暗号化情報復号部

１１０　暗号化テーブル情報復号部

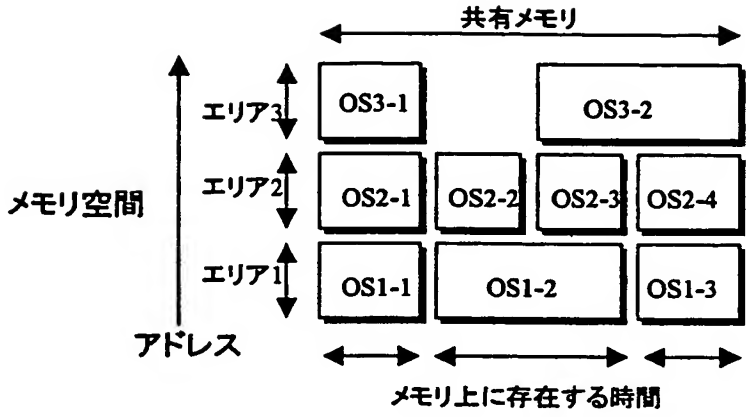
１１１　プログラム生成部

【書類名】　　図面

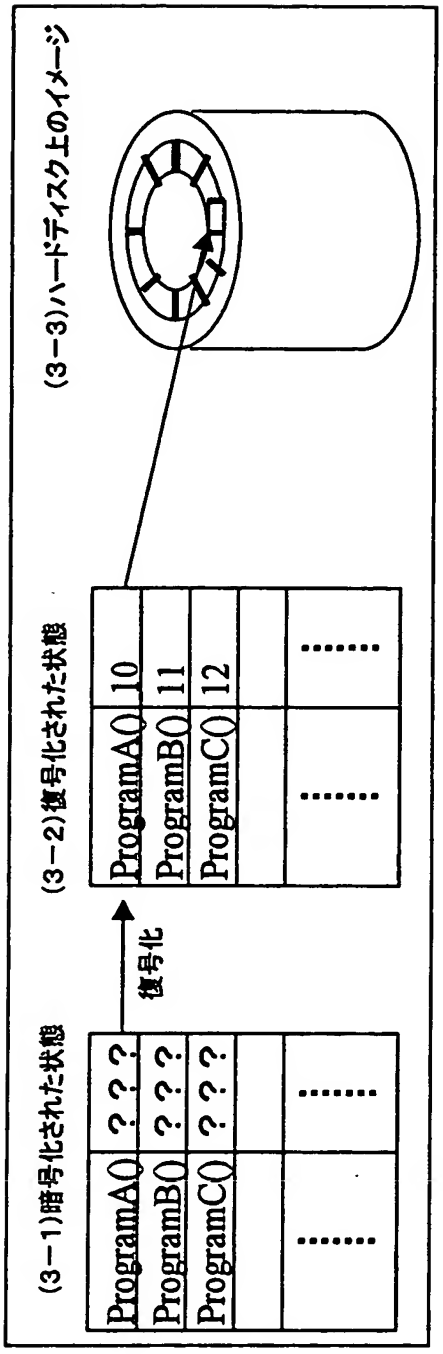
【図１】


プログラムローダ
復号支援プログラム認証部
100
暗号鍵保持部
101
暗号化データ復号部
102
暗号化テーブル情報復号部
103
アドレステーブル情報保持部
104
メモリ配置情報保持部
105
暗号化情報復号部
109
制御部
106
不正アクセス防止部
107
メモリアドレス定義部
108
アドレス情報認証部
110
プログラム生成部
111

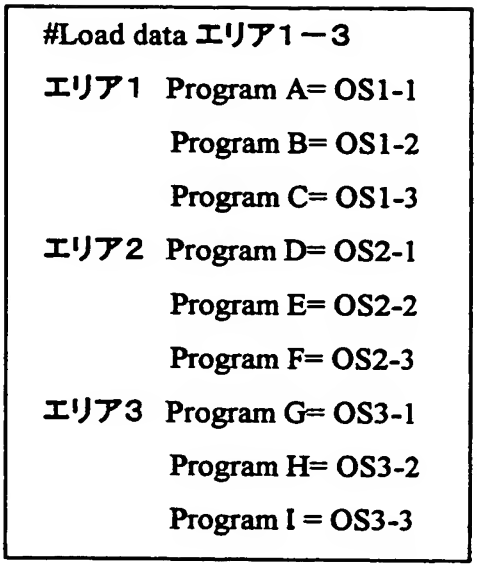
【図２】


共有メモリ
エリア3
エリア2
エリア1
メモリ空間
アドレス
OS3-1
OS3-2
OS2-1
OS2-2
OS2-3
OS2-4
OS1-1
OS1-2
OS1-3
メモリ上に存在する時間

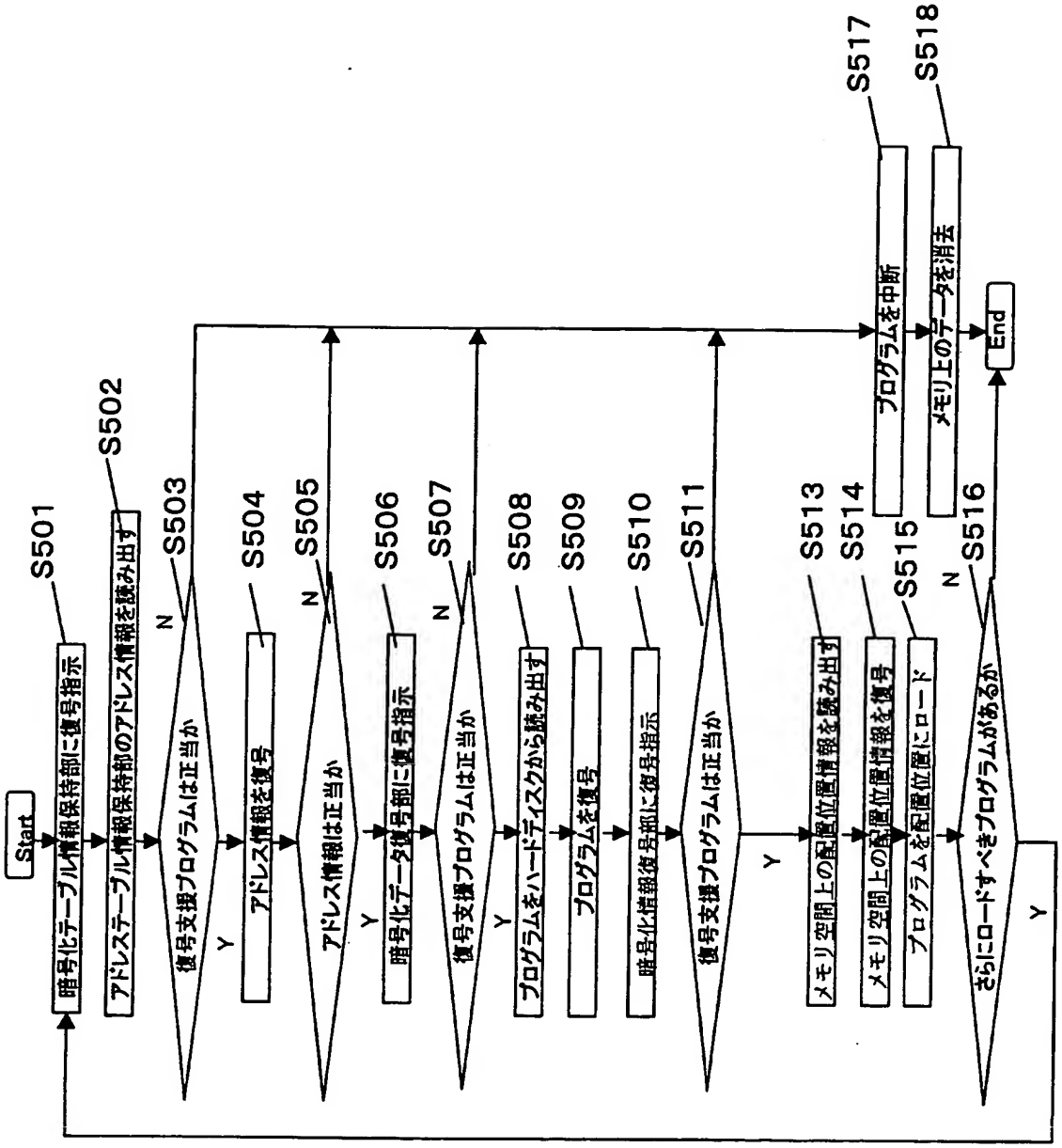
【図３】


(3－1)暗号化された状態
ProgramA() ???
ProgramB() ???
ProgramC() ???
.....
復号化
(3－2)復号化された状態
ProgramA() 10
ProgramB() 11
ProgramC() 12
.....
(3－3)ハードディスク上のイメージ

【図４】


#Load data エリア１－３
エリア１ Program A= OS1-1
Program B= OS1-2
Program C= OS1-3
エリア２ Program D= OS2-1
Program E= OS2-2
Program F= OS2-3
エリア３ Program G= OS3-1
Program H= OS3-2
Program I = OS3-3

【図５】


Start
S501
暗号化テーブル情報保持部に復号指示
S502
アドレステーブル情報保持部のアドレス情報を読み出す
S503
復号支援プログラムは正当か
N
Y
S504
アドレス情報を復号
S505
アドレス情報は正当か
N
Y
S506
暗号化データ復号部に復号指示
S507
復号支援プログラムは正当か
N
Y
S508
プログラムをハードディスクから読み出す
S509
プログラムを復号
S510
暗号化情報復号部に復号指示
S511
復号支援プログラムは正当か
Y
S513
メモリ空間上の配置位置情報を読み出す
S514
メモリ空間上の配置位置情報を復号
S515
プログラムを配置位置にロード
S516
さらにロードすべきプログラムがあるか
N
Y
S517
プログラムを中断
S518
メモリ上のデータを消去
End

【書類名】　要約書

【要約】

【課題】　仕様が公開されているオープンなコンピュータシステムにおいても、メモリ上からプログラムの全体を覗き見を防止するための暗号化プログラム復号装置を提供する。

【解決手段】　単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、制御部１０６が、暗号化データ復号部１０２と暗号化情報復号部１０９に復号指示を出し、アドレステーブル情報保持部１０３が保持する情報に従って前記プログラムを二次記憶装置上から読み出し、暗号化された前記プログラムを復号し、メモリ配置情報保持部１０４が保持する暗号化された情報をメモリ空間上の配置位置にロードすることにより、暗号化プログラムを小さな単位でメモリ上にロード可能とし、また、プログラムをロードするアドレスや、ロードされている時間をプログラムの構造やアルゴリズムによって最適化することができる。

【選択図】　図１

出 願 人 履 歴 情 報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社